Algorithmic Due Process in Criminal Justice: Transparency, Human Oversight, and the Legal Limits of AI-Assisted Judicial Decision-Making

Sergio Pommier Gallo, PhD

ORCID

0009-0000-7387-3943

Web of Science ResearcherID

QDO-1840-2026

Abstract

The increasing deployment of artificial intelligence in criminal justice is transforming the manner in which legal information is processed, risks are assessed, evidence is evaluated, and judicial decisions are supported. While existing scholarship has extensively examined algorithmic prediction, criminal liability, automated policing, and the evidentiary implications of artificial intelligence, a distinct doctrinal problem remains insufficiently differentiated: the procedural consequences of allowing algorithmic outputs to participate in criminal adjudication without adequately defined requirements of transparency, human oversight, contestability, and judicial responsibility. This article examines the emergence of algorithmic due process as a legal problem within contemporary criminal justice. It does not propose an autonomous theory of algorithmic adjudication. Instead, it conducts a doctrinal and comparative analysis of existing principles of due process, fair trial, judicial reasoning, effective remedy, equality, and human oversight as they apply to AI-assisted decision-making. Particular attention is given to the European Union Artificial Intelligence Act, the Council of Europe European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems, the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, and established procedural guarantees under European human-rights law. The analysis demonstrates that the central legal problem is not whether artificial intelligence may assist judicial institutions, but whether algorithmic assistance can remain legally subordinate to accountable human adjudication. The article argues that transparency must extend beyond technical disclosure to procedural intelligibility; human oversight must

constitute an effective capacity to reject or disregard algorithmic outputs; and judicial reasoning must remain independently attributable to the legally competent decision-maker. Algorithmic systems may therefore function as instruments of judicial assistance, but their outputs cannot displace the individualized reasoning, adversarial contestability, and institutional accountability required by criminal procedure.

Keywords: artificial intelligence; criminal justice; algorithmic due process; judicial decision-making; human oversight; transparency; explainability; fair trial; criminal procedure; judicial accountability

Introduction

Artificial intelligence is increasingly becoming part of the institutional infrastructure through which criminal justice systems process information and exercise public authority. Its applications range from document classification and legal research to evidentiary analysis, risk assessment, biometric identification, case management, and decision-support systems. The development of these technologies presents an important distinction between automation as an administrative technique and algorithmic assistance as an element of legal decision-making. The former may primarily concern efficiency. The latter directly implicates the legitimacy of the exercise of judicial power.

The legal significance of this distinction has become more pronounced as regulatory frameworks have moved from general ethical principles toward binding requirements concerning high-risk artificial intelligence. Regulation (EU) 2024/1689, commonly known as the Artificial Intelligence Act, expressly recognizes risks associated with AI systems used in law enforcement and judicial contexts, particularly where opacity, inaccurate outputs, inadequate documentation, or insufficient explainability may affect procedural rights, the presumption of innocence, the right of defence, or access to effective remedies.

The Council of Europe had already identified the structural nature of this problem through its European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment. The Charter established five principles: respect for fundamental rights, non-discrimination, quality and security, transparency and fairness, and user control. These principles are significant because they treat artificial

intelligence in judicial environments not merely as a technological innovation but as an institutional instrument whose operation must remain compatible with fundamental legal guarantees.

More recently, the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law has provided the first international legally binding treaty specifically addressing artificial intelligence through the combined framework of human rights, democracy, and the rule of law. The Convention was opened for signature on 5 September 2024 and seeks to ensure that activities within the lifecycle of AI systems remain consistent with these foundational principles.

These developments create an emerging doctrinal question. Traditional procedural law assumes that the relevant decision-maker is identifiable, institutionally accountable, and capable of providing reasons capable of adversarial examination. Algorithmic decision-support systems complicate these assumptions because their outputs may result from statistical correlations, proprietary models, complex computational processes, or training data that are not readily accessible to the parties or even fully comprehensible to the legal professional using the system.

The problem is therefore not adequately characterized as one of technological transparency alone. A criminal proceeding may satisfy a formal requirement of disclosure while still failing to provide the accused with a meaningful capacity to understand, challenge, and contest the role played by an algorithm in the decision-making process. Similarly, the existence of a human judge does not necessarily establish meaningful human control if the institutional environment creates strong incentives to defer to algorithmic recommendations.

This article examines that problem through the concept of algorithmic due process. The term is used here descriptively rather than as a claim that a new autonomous branch of procedural law has already been established. It refers to the application and progressive adaptation of established due-process guarantees to circumstances in which algorithmic systems materially contribute to criminal-justice decision-making.

Research Question

To what extent do existing principles of criminal due process, fair trial, judicial reasoning, transparency, effective remedy, and human oversight impose legal limits on the use of artificial intelligence in criminal adjudication?

Hypothesis

Where an artificial intelligence system materially contributes to a criminal-justice decision affecting an individual's rights or legal position, existing procedural guarantees require more than the formal presence of a human decision-maker. Meaningful legality requires sufficient procedural transparency to permit effective contestation, competent and independent human oversight capable of rejecting algorithmic outputs, and judicial reasoning that remains attributable to the legally authorized human decision-maker.

Theoretical Framework

The legal analysis begins from a conventional conception of criminal adjudication as an exercise of public authority constrained by procedural legality. Criminal justice does not derive legitimacy solely from the substantive correctness of its outcomes. It also depends upon the fairness of the procedure through which those outcomes are produced.

The European Convention on Human Rights provides a particularly important reference point. Article 6 protects the right to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. The provision operates within a broader procedural structure that includes equality of arms, adversarial proceedings, adequate facilities for the preparation of a defence, and reasoned judicial determination.

Artificial intelligence introduces a technological intermediary into this structure. The intermediary may not itself possess legal authority, yet its output can influence the human actor who does. The resulting problem is therefore one of institutional mediation: an algorithm may lack legal personality and judicial authority while nevertheless affecting the factual or evaluative premises upon which judicial authority is exercised.

This distinction is important. The legality of a judicial decision cannot be established merely by asking whether a human judge formally signed the decision. The relevant

inquiry must also consider whether the judge exercised genuine independent judgment and whether the parties possessed a meaningful opportunity to challenge material algorithmic inputs.

The European Ethical Charter provides a useful doctrinal starting point because it expressly connects AI use with fundamental rights, non-discrimination, quality and security, transparency, fairness, and user control. The Charter's principle of user control is especially relevant to judicial decision-making. It rejects a prescriptive conception in which the technological system determines the course of action and instead requires human users to remain informed and capable of exercising control over their decisions.

This principle can be translated into criminal procedure without creating a new doctrine. Existing judicial independence requires that the legal decision remain the product of the competent judicial authority. Accordingly, where AI is employed as a decision-support instrument, the system may inform the judge but cannot become the functional source of adjudicative authority.

The same reasoning applies to transparency. Transparency should not be reduced to publication of technical information concerning a model. Criminal procedure is concerned with the ability of the parties to understand and challenge the basis of a decision. Consequently, legally relevant transparency must be assessed according to the procedural function of information.

The distinction between technical and procedural transparency is therefore fundamental. Technical transparency may concern source code, model architecture, training datasets, performance metrics, or system documentation. Procedural transparency concerns the information necessary for the accused and other participants to determine whether and how an AI system affected the decision. The two may overlap, but they are not identical.

The EU Artificial Intelligence Act illustrates this distinction. Article 13 requires high-risk AI systems to provide sufficient transparency to enable deployers to interpret outputs appropriately, while Article 14 establishes requirements for effective human oversight. Article 86 additionally provides, under specified conditions, a right to obtain

clear and meaningful explanations concerning the role of a high-risk AI system in individual decision-making.

The emergence of these provisions confirms a broader legal development: algorithmic systems are increasingly being evaluated according to their effect upon legally protected interests rather than solely according to their technological characteristics.

Methodology

This study employs qualitative doctrinal legal research, comparative legal analysis, and normative analysis. The primary materials comprise applicable international and European legal instruments, official institutional documents, and regulatory texts concerning artificial intelligence and judicial systems.

The principal normative materials examined include the European Convention on Human Rights, Regulation (EU) 2024/1689, the Council of Europe European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment, and the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law.

The analysis proceeds through four interconnected dimensions: transparency, human oversight, contestability, and judicial accountability. These dimensions are examined not as independent technological principles but as procedural requirements derived from established legal guarantees.

The comparative component focuses principally on European regulatory developments because they currently provide one of the most developed normative frameworks for AI governance in justice. The analysis does not assume that European standards automatically constitute universal law. Rather, they are examined as evidence of an emerging regulatory direction relevant to comparative criminal-law scholarship.

Results and Legal Analysis

1. From Algorithmic Assistance to Algorithmic Due Process

The first finding is that the legal relevance of artificial intelligence in criminal proceedings depends primarily upon its functional role.

An AI system used to organize a court's administrative files presents a different legal problem from an AI system used to evaluate evidence, assess recidivism, classify defendants, or generate recommendations concerning the outcome of a criminal case. The closer the system operates to the substantive determination of a person's legal position, the greater the procedural significance of its operation.

This functional approach is consistent with the risk-based architecture of the EU Artificial Intelligence Act. Article 6 classifies specified AI systems as high-risk and expressly recognizes that high-risk classification is connected to potential harm to fundamental rights and the possibility that an AI system materially influences decision-making.

The legal consequence is that the same technological system cannot necessarily be evaluated in identical terms across institutional contexts. AI used for clerical assistance and AI used to generate a recommendation about a defendant's liberty implicate different levels of legal risk.

The central procedural question is consequently not whether an AI system is technically sophisticated. It is whether its output has sufficient normative significance to affect the rights, obligations, or legal position of a participant in criminal proceedings.

2. Transparency as a Condition of Contestability

A criminal defendant cannot meaningfully challenge an algorithmic contribution to a decision if the defendant is unaware that the system was used, does not know what function it performed, or cannot determine how its output influenced the decision.

The principle of adversarial proceedings requires practical rather than merely formal access to the relevant basis of adjudication. Consequently, algorithmic transparency must be understood relationally: information is legally relevant to the extent that it enables a participant to exercise a procedural right.

The EU AI Act's framework supports this approach. Article 13 requires transparency sufficient to allow deployers to interpret high-risk AI outputs appropriately, while Article 86 establishes a specific explanation mechanism for certain decisions based on high-risk AI systems that significantly affect individuals.

This does not mean that every criminal defendant must receive unrestricted access to source code or proprietary technical information. Such a requirement would unnecessarily equate procedural transparency with technological disclosure. The legally relevant standard is instead whether sufficient information is available to permit meaningful challenge.

At minimum, where an AI system materially contributes to a criminal decision, procedural transparency should ordinarily identify the system's use, its relevant function, the nature of the output, the material role assigned to that output, and the manner in which the human decision-maker evaluated it.

Without these elements, an accused person may face an epistemic asymmetry: the state possesses the technological and institutional capacity to rely upon the algorithm while the defendant lacks the information required to challenge it.

That asymmetry is especially problematic in criminal proceedings because the state exercises coercive authority against the individual.

3. Human Oversight Must Be Substantive

The second major finding concerns human oversight.

The mere presence of a human decision-maker is insufficient if the human actor is institutionally or psychologically predisposed to accept algorithmic recommendations. This phenomenon is commonly discussed in terms of automation bias. The EU AI Act expressly requires human oversight measures to enable designated persons to understand system limitations, detect anomalies, interpret outputs, disregard or override outputs, and, where appropriate, interrupt the system.

This requirement has direct relevance for judicial systems.

A judge who simply adopts an algorithmically generated recommendation without independently evaluating the evidentiary and legal basis of the decision is not exercising meaningful oversight. The algorithm may not possess formal legal authority, but it can acquire functional authority through institutional dependence.

The distinction can be expressed as follows:

Formal human control exists when a human legally signs or validates the decision.

Substantive human control exists when the human decision-maker possesses the competence, information, authority, and institutional independence necessary to reject the algorithmic recommendation.

Only the second form is compatible with a robust conception of judicial accountability.

The EU framework specifically requires high-risk systems to be designed so that natural persons can effectively oversee them, with oversight measures proportionate to the system's risk, autonomy, and context. The deployer obligations similarly require the assignment of human oversight to persons possessing appropriate competence, training, authority, and support.

These requirements reinforce a conventional legal principle: responsibility cannot be transferred to a technological instrument merely because that instrument contributed to the decision.

4. Judicial Reasoning Cannot Be Delegated to an Algorithm

Judicial reasoning has a distinctive legal function. It demonstrates that the decision-maker considered the relevant facts, applied the applicable law, and reached a conclusion through an intelligible process of legal reasoning.

AI-generated recommendations may assist that process, but they cannot themselves constitute judicial reasoning.

This distinction is particularly important where machine-learning systems operate through statistical inference rather than conventional legal reasoning. A model may identify correlations within large datasets without possessing an understanding of legal norms, evidentiary standards, proportionality, or the individualized circumstances of a defendant.

The resulting danger is a substitution effect: the human judge may retain formal authority while the algorithm increasingly determines the informational architecture within which the decision is made.

Such a development would be problematic even where the algorithm has high predictive accuracy. Accuracy and legality are different normative concepts.

A prediction can be statistically accurate while being legally irrelevant. Conversely, a legally relevant fact may be difficult to encode into a statistical model. Criminal adjudication requires not only prediction but legal characterization, evidentiary evaluation, procedural fairness, and individualized judgment.

The European Ethical Charter recognizes this distinction by treating AI as an instrument that must remain under user control and by requiring respect for fundamental rights, transparency, fairness, and quality.

The proper legal model is therefore assistive rather than substitutive.

5. The Presumption of Innocence and Algorithmic Risk Assessment

Algorithmic risk assessment presents a particularly sensitive application because it can influence pre-trial detention, supervision, sentencing, or other decisions concerning an individual's future conduct.

The presumption of innocence establishes a fundamental conceptual boundary. Criminal justice cannot treat a statistical prediction of future risk as equivalent to proof of past criminal conduct.

This does not necessarily prohibit risk assessment tools. It does, however, require careful differentiation between evidentiary facts concerning the charged offence and probabilistic assessments concerning future behaviour.

The EU AI Act itself recognizes the particular risks associated with AI in law enforcement. Its recitals identify potential effects on surveillance, arrest, deprivation of liberty, procedural rights, the presumption of innocence, the right of defence, and effective remedies.

Accordingly, where an algorithmic risk score materially affects liberty, the defendant should have a meaningful opportunity to contest the score's relevance, reliability, and role in the decision.

The critical question is not whether the algorithm produces a numerical output. It is whether the legal system gives that output an evidentiary status that exceeds what its methodological basis can legitimately support.

6. Fundamental Rights Impact Assessment

Another significant development is the movement from ex post remedies toward ex ante assessment.

Article 27 of the EU AI Act establishes fundamental-rights impact assessment obligations for specified deployers of high-risk AI systems. The assessment mechanism is intended to identify and address risks to fundamental rights associated with the specific context in which the system is deployed.

This approach is particularly important in criminal justice because the same system can produce different legal risks depending upon its institutional environment.

A model deployed to assist legal research does not have the same consequences as a model deployed to recommend pre-trial detention. A facial-recognition system used for a narrowly defined investigative purpose does not present precisely the same risk as a system used to determine an individual's credibility or culpability.

Context therefore becomes an element of legality.

The Council of Europe has similarly moved toward operationalization. Its 2023 Assessment Tool for the Operationalisation of the European Ethical Charter provides measures and safeguards intended to guide the procurement, design, development, implementation, and use of AI systems in judicial environments.

The doctrinal significance is substantial. AI governance in criminal justice is moving from abstract ethical principles toward institutional compliance mechanisms.

7. Effective Remedy and Algorithmic Contestability

A procedural right without a practical mechanism for contesting the technological basis of a decision may become largely formal.

Effective remedy therefore represents a central component of algorithmic due process. If an AI system materially influenced a decision affecting liberty or criminal responsibility, the affected person must possess some meaningful avenue to challenge that contribution.

This does not necessarily require a separate judicial proceeding concerning the algorithm. Existing procedural mechanisms may be sufficient where they permit the defendant to question the system's use, evidentiary relevance, reliability, and influence on the decision.

The EU AI Act's Article 85 provides a general complaint mechanism concerning infringements of the Regulation, while Article 86 creates a specific explanation right in defined circumstances. These mechanisms do not replace criminal procedural guarantees, but they illustrate the emergence of regulatory tools directed toward algorithmic contestability.

The Council of Europe's broader framework similarly places AI within the rule-of-law architecture rather than treating it solely as a technological or economic matter. The Framework Convention seeks to fill legal gaps created by rapid technological development while maintaining consistency with human rights, democracy, and the rule of law.

8. Judicial Accountability and the Problem of Responsibility Diffusion

AI-assisted adjudication may also produce responsibility diffusion.

Traditional judicial decision-making permits the identification of a responsible institution and decision-maker. Algorithmic systems introduce additional actors: software providers, data suppliers, system developers, technical auditors, institutional administrators, and procurement authorities.

The resulting chain can make it difficult to determine who is responsible when an algorithmically influenced decision is erroneous.

The EU AI Act responds to this problem by allocating distinct obligations across providers, deployers, and other actors. Article 26, for example, establishes obligations

for deployers of high-risk systems, including appropriate organizational measures and human oversight.

Nevertheless, regulatory allocation does not eliminate judicial responsibility.

A judge cannot defend an adjudicative decision merely by stating that the relevant recommendation was produced by an external system. Nor should a technological provider become the de facto adjudicator because the judicial institution lacks sufficient technical competence to evaluate the system.

Institutional responsibility must therefore remain connected to institutional authority.

Where a court possesses the legal authority to decide, it must retain sufficient operational and epistemic capacity to exercise that authority responsibly.

9. Algorithmic Literacy as a Procedural Competence

Effective human oversight presupposes competence.

The EU AI Act recognizes the importance of AI literacy in assigning responsibilities to persons overseeing high-risk AI systems. For judicial institutions, this principle has a particularly important implication: judicial independence in an algorithmic environment increasingly requires technological competence sufficient to evaluate the limitations of decision-support systems.

This does not mean that judges must become software engineers.

Rather, they must understand the legally relevant characteristics of the systems they use: what the system is designed to do, what it cannot reliably do, what data it processes, what forms of uncertainty accompany its output, and under what circumstances the output should not be relied upon.

Without such competence, human oversight may become symbolic.

Algorithmic literacy should therefore be regarded as an institutional component of responsible judicial modernization. It protects not only defendants but also judges,

because it reduces the risk that judicial actors will unknowingly delegate substantive judgment to systems whose limitations they cannot adequately assess.

Discussion

The analysis demonstrates that the emerging legal framework does not require criminal justice systems to reject artificial intelligence. Neither the Council of Europe's ethical framework nor the EU regulatory model adopts such a position. The CEPEJ expressly recognizes that AI may improve the efficiency and quality of justice, while insisting that its deployment remain compatible with fundamental rights and under meaningful human control.

The central legal issue is therefore institutional design.

AI may legitimately support judicial work where its role remains subordinate to legal judgment, procedural rights remain effective, and the decision-maker retains meaningful control. Conversely, the legal legitimacy of AI-assisted adjudication becomes increasingly difficult to defend where algorithmic outputs are opaque, materially determinative, effectively unchallengeable, or treated as authoritative because of their technological status.

Four principles emerge from the doctrinal analysis.

First, **algorithmic transparency must be procedural rather than merely technical**. The relevant question is whether the parties can understand the system's role sufficiently to exercise their procedural rights.

Second, **human oversight must be effective rather than ceremonial**. A human actor must possess the authority and competence to reject, disregard, or override an algorithmic output.

Third, **judicial reasoning must remain independently attributable to the judge**. An algorithm cannot become a concealed substitute for judicial reasoning.

Fourth, **effective remedy must encompass meaningful algorithmic contestability** where an AI system materially affects a person's legal position.

These principles do not constitute a new autonomous theory of criminal adjudication. They are instead an application of established procedural concepts to a changed technological environment.

This distinction is important for doctrinal stability. Criminal procedure has historically adapted to new technologies without abandoning its fundamental principles. The emergence of forensic science, electronic evidence, digital communications, DNA analysis, and computerized databases all required procedural adaptation. Artificial intelligence represents a further stage in this process.

Its distinctive feature is not simply that it processes information electronically. It is that certain systems generate classifications, predictions, recommendations, or other outputs that may influence human judgments.

The legal system must consequently preserve the boundary between information processing and the exercise of adjudicative authority.

The European regulatory developments examined here indicate a gradual movement toward this objective. The EU AI Act introduces binding requirements concerning high-risk AI systems, including transparency, human oversight, deployer responsibilities, and specified explanation rights. The Council of Europe supplements this regulatory direction through its Ethical Charter, its operational assessment tool, and its Framework Convention.

At the same time, these instruments should not be understood as replacing national criminal procedure or the European Convention on Human Rights. Their significance lies in establishing additional governance requirements that interact with existing procedural safeguards.

The strongest legal position is therefore one of integration rather than replacement.

Algorithmic governance should operate within criminal procedure, not outside it.

Limitations

This study has several limitations.

First, the regulatory landscape surrounding artificial intelligence remains dynamic. The EU Artificial Intelligence Act establishes a phased regulatory architecture, and its practical implementation will continue to generate interpretative guidance and institutional practice. The analysis therefore focuses on established legal provisions rather than attempting to predict future regulatory developments.

Second, the comparative analysis concentrates principally on European instruments because they provide an unusually developed legal framework for AI and justice. The conclusions should not automatically be treated as statements of positive law in jurisdictions outside that framework.

Third, the study is doctrinal rather than empirical. It does not measure the actual frequency with which judges rely upon AI systems, nor does it assess the statistical accuracy of particular technologies.

Fourth, algorithmic systems differ substantially in architecture, purpose, data sources, and degree of autonomy. The legal assessment must therefore remain contextual. No single procedural rule can be assumed to apply identically to every AI application used within criminal justice.

These limitations do not undermine the central conclusion. They reinforce the necessity of evaluating algorithmic systems according to their actual institutional function and legal consequences.

Conclusions

Artificial intelligence is becoming an increasingly significant component of contemporary criminal justice, but its incorporation into judicial systems does not displace the procedural principles that traditionally constrain criminal adjudication.

The principal legal challenge is not technological autonomy in the abstract. It is the possibility that algorithmic outputs may acquire practical authority without corresponding procedural transparency, contestability, and institutional accountability.

The emerging European framework demonstrates that this risk is already recognized in positive regulatory and institutional instruments. The EU Artificial Intelligence Act

imposes requirements concerning high-risk systems, transparency, human oversight, deployer responsibility, and explanation rights. The Council of Europe's Ethical Charter establishes fundamental rights, non-discrimination, quality, security, transparency, fairness, and user control as core principles for AI in judicial environments. The Council of Europe Framework Convention extends the normative framework by connecting AI governance with human rights, democracy, and the rule of law.

These developments support a legally conservative conclusion.

Artificial intelligence may assist criminal adjudication, but it cannot legitimately become an undisclosed substitute for judicial reasoning. Its outputs may inform a decision, but they cannot acquire independent adjudicative authority. Human oversight must be sufficiently substantive to permit rejection or reversal of algorithmic recommendations. Transparency must enable meaningful procedural challenge rather than merely satisfy technical disclosure requirements. And where algorithmic processing materially affects a person's legal position, effective remedies must include the practical ability to contest the system's role and output.

The concept of algorithmic due process therefore emerges not as a wholly new doctrine, but as a necessary application of established procedural guarantees to a technologically transformed decision-making environment.

The fundamental principle remains straightforward: **technological assistance may modernize the administration of criminal justice, but it cannot displace the legal responsibility of the institution empowered to adjudicate.**

The future legitimacy of AI-assisted criminal justice will consequently depend less upon the sophistication of algorithms than upon the capacity of legal institutions to preserve the distinction between computational assistance and judicial authority.

References

Council of Europe. (2018). *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*. European Commission for the Efficiency of Justice.

Council of Europe. (2023). *Assessment Tool for the Operationalisation of the European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*. European Commission for the Efficiency of Justice.

Council of Europe. (2024). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS No. 225).

European Court of Human Rights. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms*. Council of Europe.

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union, L 119*, 1–88.

European Parliament & Council of the European Union. (2016). Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. *Official Journal of the European Union, L 119*, 89–131.

European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*.

European Commission for the Efficiency of Justice. (2018). *European Ethical Charter on the use of artificial intelligence in judicial systems and their environment*. Council of Europe.

Council of Europe. (2024). *Explanatory Report to the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*.

Susskind, R. (2019). *Online Courts and the Future of Justice*. Oxford University Press.

Zalnieriute, M., Moses, L. B., & Williams, G. (2019). The rule of law and automation of government decision-making. *Modern Law Review, 82*(3), 425–455.

Surden, H. (2019). Artificial intelligence and law: An overview. *Georgia State University Law Review, 35*(4), 1305–1338.

Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. *University of Pennsylvania Law Review, 165*(3), 633–705.

Citron, D. K., & Pasquale, F. (2011). The scored society: Due process for automated predictions. *Washington Law Review, 89*, 1–33.

Council of Europe. (2025). *Artificial intelligence and justice: Cyberjustice and artificial intelligence resources*. European Commission for the Efficiency of Justice.